СИСТЕМА ВИРТУАЛИЗАЦИИ ДЛЯ WINDOWS-СИСТЕМ НА ОСНОВЕ ГИПЕРВИЗОРА HYPER-V

Прокопюк С.Ю., Цыганков Ю.В.
Томский политехнический университет
Jedi4334@gmail.com

Введение

Клиентская виртуализация становится все более востребованной функцией, причем не только у IT специалистов, но и среди обычных пользователей для кроссплатформенных разработок, тестирования, или если хочется испытать ОС, но нет возможности ее прямой установки. У компании Microsoft долгое время не было достойного решения в этой области, поэтому для клиентской виртуализации приходилось использовать сторонние приложения, такие как Oracle VirtualBox или VMWare Workstation.

С появлением нового ядра vNext и выходом Windows 8, а затем и Windows 10 ситуация изменилась в лучшую сторону. Пользуясь тем, что Windows 8 базируется на одном ядре с Windows Server 2012, в Microsoft взяли серверную роль Hyper-V и с минимальными изменениями перенесли ее в клиентскую операционную систему, назвав новый функционал клиентским гипервизором (Client Hyper-V).

Системные требования:

- ***Процессор*** – Для работы Hyper-V необходим 64-битный процессор производства Intel или AMD с поддержкой инструкций NX и SSE2. Процессор должен поддерживать технологии виртуализации (Intel VT-x или AMD-V), а также технологию преобразования адресов второго уровня (Second Level Address Translation, SLAT).
- ***Оперативная память*** – Согласно рекомендациям Microsoft, для работы Hyper-V необходимо минимум 4Гб оперативной памяти. На этом объеме ОЗУ вы сможете стартовать основную систему и запустить максимум одну-две нетребовательных к памяти виртуальных систем. Для более-менее комфортной работы стоит рассчитывать минимум на 8Гб ОЗУ. Максимум аппаратная поддержка же практически не ограничен, так как как сам Hyper-V поддерживает выделение до 512Гб ОЗУ для одной ВМ – все зависит от финансовых возможностей.
- ***Дисковая подсистема*** – Hyper-V предъявляет довольно серьезные требования к производительности дисковой подсистемы. Если вы планируете запускать одновременно несколько ВМ, то стоит подумать о том, чтобы выделить под них отдельный жесткий диск, либо организовать RAID. Впрочем, жестких ограничений нет и при желании виртуальные машины можно хранить где угодно, например на Flash накопителе или в сетевом хранилище но нужно быть готовым к крейе медлительной работе ВС. Версия ядра 2016 позволяет выносить виртуальную машину в облако Azure, но для работы нужно стабильное и высокоскоростное соединение с сетью Интернет.
- ***Операционная система*** – В качестве операционной системы для Hyper-V можно использовать только 64-битные версии Windows 8\8.1\10, редакций Professional или Enterprise.

Принцип работы

Архитектура Hyper-V представлена на рисунке 1.

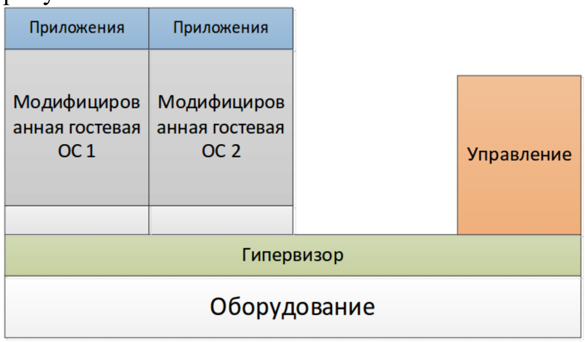

Рис.1. Архитектура Hyper-V

Раздел — логическая единица разграничения, поддерживаемая гипервизором, в котором работают операционные системы. Hyper-V разграничивает системы согласно понятию раздел.

Принцип физического доступа к оборудованию представлен на рисунке 2. Виртуализированные разделы не имеют ни доступа к физическому процессору, ни возможности управлять его реальными прерываниями. Вместо этого, у них есть виртуальное представление процессора и гостевой виртуальный адрес, зависящий от конфигурации гипервизора, вовсе необязательно при этом занимающий все виртуальное адресное пространство [1]. Дочерние разделы не имеют непосредственного доступа к аппаратным ресурсам, но зато получают виртуальное представление ресурсов, называемое виртуальными устройствами. Любая попытка обращения к виртуальным устройствам перенаправляется через VMBus к устройствам родительского раздела, которые и обработают данный запрос. VMBus — это логический канал, осуществляющий взаимодействие между разделами. Ответ возвращается также через VMBus. Если устройства родительского раздела также являются виртуальными устройствами, то запрос будет передаваться дальше пока не достигнет такого родительского раздела, где он получит доступ к физическим устройствам. Родительские разделы запускают провайдер сервиса виртуализации (Virtualization Service Provider или сокр. VSP) который соединяется с VMBus и обрабатывает запросы доступа к устройствам от дочерних разделов. Виртуальные устройства дочернего раздела работают с клиентом сервиса виртуализации (Virtualization Service Client или сокр. VSC), который перенаправляет запрос через VMBus к VSP родительского раздела. Этот процесс прозрачен для гостевой ОС [2].

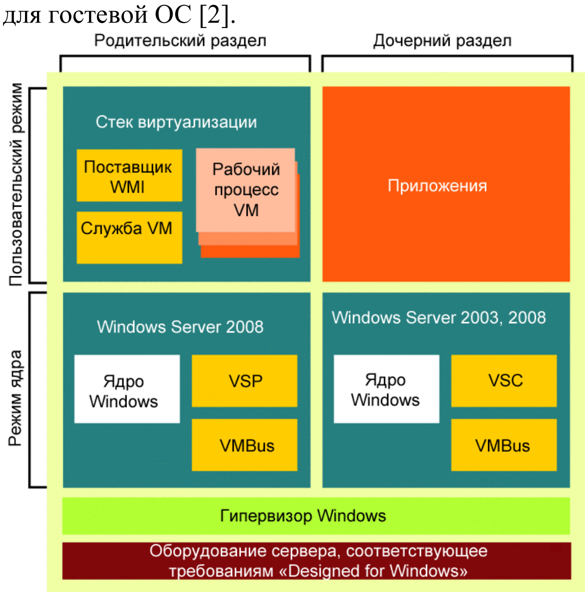

Рис. 2. Управление доступом к физическому оборудованию

Ядро системы

Микроядерная архитектура, представленная на рисунке 3, разработана для минимизации области, открытой для атак и улучшения безопасности, особенно при применении Hyper-V в роли ядра сервера.

Микроядерный подход использует очень тонкий, специализированный гипервизор, выполняющий лишь основные задачи обеспечения изоляции разделов и управления памятью. Этот уровень не включает стека ввода/вывода или драйверов устройств. Это подход, используемый Hyper-V. В этой архитектуре стек виртуализации и драйверы конкретных устройств расположены в специальном разделе, именуемом родительским разделом.

Server Core («ядро сервера») – это вариант установки Windows Server 2008. Гипервизор не содержит драйверов устройств или кода от сторонних производителей, предоставляя более стабильный, тонкий и безопасный фундамент для работы виртуальных компьютеров. Hyper-V также предоставляет прочную безопасность на основе ролей, с помощь интеграции Active Directory. Вдобавок, Hyper-V позволяет виртуальным компьютерам пользоваться преимуществами функций безопасности уровня оборудования, таких как фрагмент исполнения отключения (NX), для повышения безопасности виртуальных компьютеров[2].

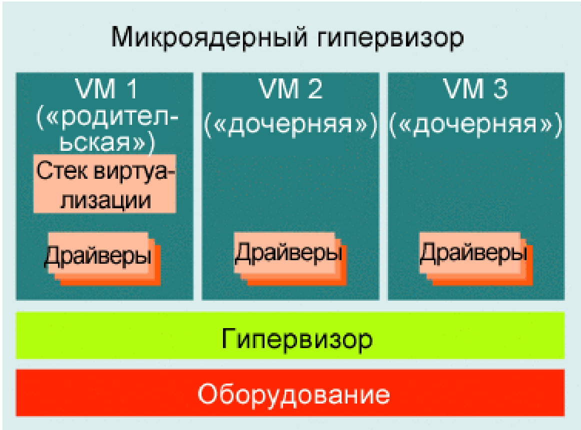

Рис.3. Модель ядра Hyper-V

Так же в Hyper-V предусмотрена защита ресурсов узла. Эта функция заимствована из Microsoft Azure; она защищает ресурсы узла Hyper-V от виртуальных машин, которые пытаются атаковать структуру, например формируя высокие рабочие нагрузки для процессора. Защита ресурсов узла динамически идентифицирует виртуальные машины, которые ведут себя «не по правилам», и уменьшает выделяемые им ресурсы.

В новой версии ядра добавлена функция защиты виртуальных машин Shielded VM. Защищенные виртуальные машины Shielded VM могут функционировать только в структурах, назначенных владельцами виртуальных машин. Защищенные виртуальные машины должны быть зашифрованы с использованием Bitlocker (или другого решения), чтобы гарантировать запуск [3].

Список литературы:

1. Hyper-V // Wikipedia // URL: https://ru.wikipedia.org/wiki/Hyper-V // Дата обращения: 14.10.15
2. Представляем Hyper-V в Windows Server 2008 // Новостной портал TechNet // URL: https://technet.microsoft.com/ru-ru/magazine/2008.10.hyperv.aspx#id0110011 // Дата обращения: 14.10.15
3. Новшества в Windows Server 2016 Hyper-V // Новостной портал NeroHelp// URL: http://nerohelp.info/6973-wm16-hyper-v-new.html // Дата обращения 18.10.15